Attorney Docket No. 1454.1512

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Christian CORRELL et al.

Serial No. 10/720,743 Group Art Unit: 2132

Confirmation No. 3113

Filed: November 25, 2003 Examiner: Venkatanaray Perungavoor

For: METHOD AND SYSTEM FOR ENCRYPTING TRANSMISSIONS OF COMMUNICATION DATA STREAMS VIA A PACKET-ORIENTED COMMUNICATION NETWORK

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

I. REAL PARTY IN INTEREST

The real party in interest is SIEMENS AKTIENGESELLSCHAFT. The inventors Christian CORRELL and Karl KLUG, assigned all rights in the subject application to SIEMENS AKTIENGESELLSCHAFT, according to the Assignment submitted for recordation on April 19, 2004 and recorded at Reel 015231, Frame 0996 on April 19, 2004.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences known to Appellants, Appellants' legal representatives or the Assignee, SIEMENS AKTIENGESELLSCHAFT, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-8 are pending in the application and stand rejected under 35 U.S.C. § 103(a).

IV. STATUS OF AMENDMENTS

No Amendment was filed in response to the September 19, 2007 final Office Action.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present application is directed to a method and apparatus for encrypting communication streams, transmitted as a sequence of data packets using the Internet Protocol (hereinafter referred to as "Internet Protocol data packets" or simply "IP data packets"). This is accomplished by either the method of claim 1 or the apparatus of claim 5 submitted on November 25, 2003. Support for the limitations recited in claims 1 and 5 can be found, *e.g.*, on pages 2-7 of the specification with reference to FIGS. 1-2 as described in detail below.

Independent claim 1 recites a method that includes "forming collective Internet Protocol data packets, each containing several Internet Protocol data packets of different communication data streams" at lines 3-4, as described in the specification, for example, on page 2, lines 25-29, page 3, lines 4-21, page 5, lines 6-13, page 5, line 20 to page 6, line 18 and page 6, line 27 to page 7, line 11 with reference to FIG. 2.

Independent claim 1 further recites, at lines 5-6, "encrypting each collective Internet Protocol data packet by an encryption module to form encrypted collective Internet Protocol data packets" as described in the specification, for example, on page 5, lines 14-19 and page 6, line 19 to page 7, line 16 with reference to FIG. 2.

Independent claim 1 finally recites "transmitting the encrypted collective Internet Protocol data packets via the packet-oriented communication network" in the last two lines and as described in the specification, for example, on page 3, lines 4-21 and page 4, line 5 to page 5, line 5, with reference to FIG. 1.

Independent claim 5 recites an apparatus that includes "a collective packet generator forming collective Internet Protocol data packets, each containing several Internet Protocol data packets of different communication data streams" at lines 4-5, as described in the specification, for example, on page 2, lines 25-29, page 3, lines 4-21, page 5, lines 6-13, page 5, line 20 to page 6, line 18 and page 6, line 27 to page 7, line 11 with reference to FIG. 2.

Independent claim 5 further recites, at lines 6-7, "an encryption module encrypting at least one of the collective Internet Protocol data packets" as described in the specification, for example, on page 5, lines 14-19 and page 6, line 19 to page 7, line 16 with reference to FIG. 2.

Independent claim 5 finally recites "an Internet Protocol interface transmitting encrypted collective Internet Protocol data packets via the communication network" in the last two lines and as described in the specification, for example, on page 3, lines 4-21 and page 4, line 5 to page 5, line 5, with reference to FIG. 1.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

In the final Office Action dated September 19, 2007, the Examiner rejected claims 1, 5 and 6 under 35 U.S.C. § 103(a) as being unpatentable over Masuda (U.S. Patent 6,931,025) in view of Aziz (U.S. Patent 6,091,820) and rejected claims 2-4, 7 and 8 under 35 U.S.C. § 103(a) as being unpatentable over Masuda and Aziz in further view of Ho et al. (U.S. Patent Publication 2003/0133461). At issue is whether Masuda, Aziz and Ho et al., alone or in combination, teaches or suggests all the limitations recited in claims 1-8.

VII. ARGUMENT

Rejection of Claims 1, 5 and 6 under 35 U.S.C. § 103(a):

The final Office Action dated September 19, 2007 rejected claims 1, 5 and 6 under 35 U.S.C. § 103(a) as being unpatentable over Masuda (U.S. Patent 6,931,025) in view of Aziz (U.S. Patent 6,091,820). Independent claims 1 and 5 each recites "forming collective Internet Protocol data packets, each containing several Internet Protocol data packets of different communication data streams" (*e.g.* claim 1, lines 4-5). In light of the intrinsic evidence offered by the specification, the phrase "collective Internet Protocol data packets" must be interpreted to be an IP data packet and is distinguishable from what is taught by Masuda as modified by Aziz.

In *Phillips v. AWH Corp.*, the Federal Circuit held that "[i]n light of the statutory directive that the inventor provide a 'full' and 'exact' description of the claimed invention, the specification necessarily informs the proper construction of the claims." *Phillips v. AWH Corp*, 75 USPQ2d 1231, 1238. Thus, the specification should be consulted when determining the scope of a term in the claims and particularly when the term does not have a common meaning in the art. The phrase "collective Internet Protocol data packets" as recited above in claims 1 and 5 is defined in the specification as "collective IP data packet SP is a conventional IP data packet in accordance with the Internet protocol with an IP packet header HDR and a usable data area, in which the individual IP data packets DP1,...,DP4 are inserted as a whole, i.e., including their particular packet headers" on page 6 lines 12-15. In particular, as described in the specification with reference to FIG. 2, "all the... IP data packets DP1,...,DP4 are assembled by the collective packet generator SPE to form a collective IP data packet SP, that is transmitted to the encryption module IPSEC" (page 6, lines 4-6) where "encryption module IPSEC is used to encrypt single IP data packets" (page (page 5, line 14). Hence, each "collective Internet Protocol data packet" is a single IP data packet "containing several Internet Protocol data packets of different communication data streams" as recited in the claims (claims 1 and 5, lines 4-5).

The significance of identifying a "collective Internet Protocol data packet" as an IP data packet is clear when put in the context of how data packets are formed in a telecommunications packet-based network. Each IP data packet inherently has additional information header information added as overhead to the transmitted payload information. This header information is applied to each and every IP data packet and constitutes an essential component of the IP data packet. Thus, a "collective Internet Protocol data packet" would have header information for each of the IP data packets representing a communication stream payload as well as additional header information for the "collective Internet Protocol data packet", where the payload for the "collective Internet Protocol data packet" would constitute aggregated IP data packets of the different communications streams.

In contrast, Masuda is directed to "[a]n optical network with an optical adaptation layer whose order is higher than synchronous optical network (SONET) layer and lower than Internet protocol (IP) layer" (Abstract, lines 1-3). In rejecting claims 1 and 5, the Office Action relied on item 3a in FIG. 4 of Masuda as teaching "forming collective Internet Protocol data packets, each containing several Internet Protocol data packets of different communication data streams" as recited in the claims (claims 1 and 5, lines 4-5). The Office Action does not describe how item 3a of FIG. 4 teaches or suggests the quoted limitation of the claims.

Therefore, in the paragraphs that follow, the Applicants will put item 3a of FIG. 4 in the proper context.

Masuda states that

> shown in FIG. 3, at each node, **optical adaptation (optical ADP) layer 2b as an intermediate layer is laid between IP layer 2a as layer 3 and SONET (synchronous optical network) layer 2c as layer 2**. Optical edge node EN terminates IP packet 2e from subscriber network la, grouping the separate IP packet 2e at optical ADP layer 2b, constructing the optical adaptation frame. In constructing the optical adaptation frame, the QOS processing or transfer determination processing in the network can be simplified by aggregating into destination network node (egress node to exit from the network to the destination user network) and QOS (for delay-oriented and best-effort).

(column 4, lines 7-19, emphasis added). Thus, the optical ADP layer taught by Masuda (2b in FIG. 3) is situated between the IP layer and the SONET layer. In addition, Masuda refers to the layers of the Open Systems Interconnect (OSI) Reference Model, developed by the International Organization of Standards, in reference to FIG. 3. The OSI Reference Model is described as "the only internationally accepted framework of standards for communications between different systems made by different vendors" (Newton's Telecom Dictionary, 20th Edition, see the Evidence Appendix). As noted in Masuda, the IP layer is in layer 3 of the OSI Reference Model, where layer 3 is described as the Network Layer and "determines how data is transferred between computers ... [it] also addresses routing within and between individual networks" (*ibid.*). In contrast, SONET is described by Masuda as being in layer 2 of the OSI Reference Model, where layer 2 is the Data Link layer and "concerned with procedures and protocols for operating the communication lines" (*ibid.*). In addition, Masuda indicates the distinction between layer 2 and layer 3 communications, by the distinct use of the word "frame", as in "optical adaptation frame" quoted above, when describing the ADP layer and "IP packet" when referring to what the "optical adaptation frame" contains. Furthermore, this discussion in Masuda regarding the distinctions between layer 2 protocols and the IP data packet agrees with the definition and discussion of an IP data packet on page 3, lines 4-10 of the specification.

Clearly, in light of both the definitions provided by the specification and Masuda with respect to the embodiment of Masuda discussed above, one skilled in the art would understand that because optical ADP layer 2b is "an intermediate layer ... laid between IP layer 2a as layer 3 and SONET ... layer 2c as layer 2" of the OSI Reference Model, the optical ADP layer is separate from layers 2 and 3. Thus, one skilled in the art would view the optical ADP layer as an additional layer to the layers contemplated by the OSI Reference Model and therefore not a part of either layer 2 or layer 3 of the OSI Reference Model.

With respect to FIG. 4, Masuda teaches "at an edge node of [the] optical network, IP packets 3f directed to ... [the] same destination are grouped, and a[n] optical ADP frame 3a to which the respective packets are aggregated is constructed" (column 4, line 65 to column 5, line 1). Thus, FIG. 4 of Masuda shows that IP packets, residing in layer 3 of the OSI Reference Model, are passed to the optical ADP layer and aggregated and then these aggregated optical frames are passed on to layer 2 of the OSI Reference Model.

As stated above, claims 1 and 5 each recites "forming collective Internet Protocol data packets, each containing several Internet Protocol data packets of different communication data streams" at lines 4-5. Since each collective IP data packet contains "several Internet Protocol data packets of different communication data streams" and the collective IP data packet is simply an IP data packet according to the definition provided by the specification, the collective IP data packet is distinguishable from an "optical ADP frame 3a [in]to which the respective [IP] packets are aggregated" as taught by Masuda. Moreover, the "ADP frame is created in a layer situated between the IP layer and the SONET layer and the arrangement of header information would be different when comparing an "optical ADP frame" described in Masuda and a "collective Internet Protocol data packet" recited in claims 1 and 5. For example, illustrated in FIG. 2 is an embodiment where "the collective IP data packet SP is a conventional IP data packet in accordance with the Internet protocol with an IP packet header HDR and a usable data area, in which the individual IP data packets DP1,...,DP4 are inserted as a whole, i.e., including their particular packet headers" (page 6, lines 12-15). In contrast with FIG. 2, FIG. 4 of Masuda illustrates an optical ADP frame as 3a and optical frame header 3b, but is silent with respect to the IP data packet header that is required to form a "collective Internet Protocol data packet" as recited in the claims.

As a consequence of how the term "collective Internet Protocol data packet" is defined in the specification, one skilled in the art would not view what is recited in the claims as being taught by what is described in Masuda because one of ordinary skill in the art would understand that the "collective Internet Protocol data packets" are formed in the IP layer 2a, not in a separate optical ADP layer 2b. As described in Masuda, what is formed in the optical ADP frame, which is not an IP data packet (like the collective IP data packet as defined in the specification), because the optical ADP frame has an ADP frame header, which does not contain an IP data packet header inherent to an IP data packet, as illustrated in FIG. 4.

On page 2, numbered paragraph 2, of the final Office Action, the Examiner suggests that since Masuda teaches an "optical node containing pluralistic subscriber network[s] such as IP" in column 3, lines 27-31, the claims do not distinguish over Masuda. Since the OSI Reference Model refers to a layering of different protocols, the optical node taught by Masuda and relied on by the Examiner, encapsulates different protocols (including the Internet Protocol) within a single optical frame. What is not described in column 3, lines 27-31 or anywhere else in Masuda is "forming collective Internet Protocol data packets" where each IP data packets "contain[s] several Internet Protocol data packets of different communication data streams" (*e.g.*, claim 1, lines 4-5). In addition, nothing has been cited in either Aziz (or Ho et al.) that would suggest modification of Masuda to provide this feature as recited in claims 1 and 5.

The final Office Action, in addition to the technical failures of the prior art described above, also failed to consider the secondary considerations enumerated by the Supreme Court in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 and affirmed in *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, ___, 82 USPQ2d 1385, 1396 (2007). In particular, the Supreme Court held:

> In *Graham v. John Deere Co. of Kansas City*, 383 U. S. 1 (1966), the Court set out a framework for applying the statutory language of §103, language itself based on the logic of the earlier decision in *Hotchkiss v. Greenwood*, 11 How. 248 (1851), and its progeny. See 383 U. S., at 15–17. The analysis is objective:

> > "Under §103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented." ...
>
> While the sequence of these questions might be reordered in any particular case, the factors continue to define the inquiry that controls.

(*KSR,* 550 U.S. at ___, 82 USPQ2d at 1391, quoting from *Graham* at 17–18). The specification of the present application clearly describes the secondary considerations that should be considered in light *KSR*. Specifically, the specification describes the benefits of combining multiple IP data packets within a single IP data packet compared to the approach of Massuda, *i.e.* combining multiple data packets into a single frame at a layer of processing subsequent to the formation of IP data packets, on page 2, line 16 to page 3, line 21 of the specification. Furthermore, the specification states:

> In accordance with an advantageous form of embodiment of the invention, the collective IP data packets can be transmitted by an encrypted tunneling method on the network layer, i.e., layer 3 of the OSI reference model. The encryption model can have an encapsulation module to encapsulate in a second IP data packet data encrypted in the encryption module of a first IP data packet. Compared with the protocols, such as PPTP, L2F or L2TP active on layer 2 of the OSI reference model, an encryption protocol active on the network layer is substantially more secure

on page 5, lines 4-10. The specification further states, with reference to the embodiment illustrated in FIG. 2, that the "insertion of complete IP data packets DP1,...,DP4 is advantageous insofar as the packet headers can also be encrypted during the subsequent encryption, so that no information regarding the origin, destination or connecting parameters of the individual communication data streams can be read by unauthorized persons" on page 6, lines 15-18. By forming the optical ADP frame in an OSI Reference Model layer outside the IP layer, Masuda modified by Aziz would be less secure then what is recited in claims 1 and 5 and requires an economically inefficient storage of the same IP data packet in both the IP layer 2a and the optical ADP layer 2b, compared to the claimed "collective Internet Protocol data packets" formed in the IP layer 2a. Thus, claims 1 and 5 each offer both technical and economical benefits not found in the prior art.

In view of the above, it is submitted that Masuda and Aziz (with or without Ho et al.), individually or in combination, do not teach all the features recited in claims 1 and 5. Claim 6 depends on claim 5, and for the reasons discussed above, it is submitted that claim 6 is patentably distinguishable over Masuda and Aziz (with or without Ho et al.).

Rejection of Claims 2-4, 7 and 8 under 35 U.S.C. § 103(a)

The final Office Action dated September 19, 2007 rejected claims 2-4, 7 and 8 under 35 U.S.C. § 103(a) as being unpatentable over Masuda and Aziz in further view of Ho et al.

Claims 2-4, 7 and 8 each depend on one of claims 1 and 5 and it is submitted that claims 2-4, 7 and 8 are patentably distinguishable over Masuda, Aziz, and Ho et al., individually or in combination, for the reasons discussed above with respect to claims 1 and 5.

Summary of Arguments

For the reasons set forth above, it is submitted that claims 1-8 patentably distinguish over Masuda, Aziz, and Ho et al., alone or in combination. Thus, it is respectfully submitted that the Examiner's rejections of the claims is without support and, therefore, erroneous. Accordingly, the Board of Patent Appeals and Interferences is respectfully urged to so find and to reverse the Examiner's rejections.

Please charge any required fee to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: March 19, 2008

By: David Moore
David E. Moore
Registration No. 59,047

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

VIII. CLAIMS APPENDIX

1. A method for encrypted transmission of communication data streams, present as a sequence of IP data packets, via a packet-oriented communication network, comprising:

forming collective Internet Protocol data packets, each containing several Internet Protocol data packets of different communication data streams;

encrypting each collective Internet Protocol data packet by an encryption module to form encrypted collective Internet Protocol data packets; and

transmitting the encrypted collective Internet Protocol data packets via the packet-oriented communication network.

2. A method in accordance with claim 1, wherein the encrypted collective Internet Protocol data packets are transmitted by an encrypted tunneling method on a network layer of an OSI reference model.

3. A method in accordance with claim 2, wherein said forming comprises:

determining which of the different communication data streams have a common transmission destination, and

forming at least one collective Internet Protocol data packet from Internet Protocol data packets of communication data streams with a common transmission destination.

4. A method in accordance with claim 3, wherein said determining and forming are performed on the Internet Protocol data packets of the different communication data streams that occur within a specified time interval.

5. A transmission device for encrypted transmission of communication data steams present in each case as a sequence of Internet Protocol data packets via a packet-oriented communication network, comprising:

a collective packet generator forming collective Internet Protocol data packets, each containing several Internet Protocol data packets of different communication data streams;

an encryption module encrypting at least one of the collective Internet Protocol data packets; and

an Internet Protocol interface transmitting encrypted collective Internet Protocol data packets via the communication network.

6. A transmission device in accordance with claim 5, wherein said encryption module includes an encapsulation module encapsulating data of a first Internet Protocol data packet encrypted in the encryption module into a second Internet Protocol data packet.

7. A transmission device in accordance with claim 6, wherein said collective packet generator comprises:

an address comparison device determining which of the different communication data streams have a common transmission destination; and

a collective packet generation device forming the collective Internet Protocol data packets, each containing Internet Protocol data packets of the different communication data streams having the common transmission destination.

8. A transmission device in accordance with claim 7, further comprising a timer for setting a time interval, with the Internet Protocol data packets of the different communication data streams that occur within the time interval being combined to form a collective Internet Protocol data packet.

IX. EVIDENCE APPENDIX

Exhibit A of the Response file August 15, 2007: Newton's Telecom Dictionary, 20th Edition, pages 603-604.

X. RELATED PROCEEDINGS APPENDIX

(None)

Exhibit A

g with rope in mind.
l Spectrum. OPTIS is a modulation tech
er Line). See also HDSL2.
hich converts electrical energy to optical
ceivers in fiber optic communications sys

and devices associated with fiber optic
no practical optical computers, all
, opto-electronic light sources convert the
hich is transmitted to the receiving
al signal. In fiber optic systems, the light
itting Diodes) or laser diodes. The
oto-INtrinsic diodes or APDs (Avalanche
d in high-speed, long-haul networks.
r short-haul, relatively low-speed
ctronic devices, repeat the optical
 light detector, convert it to electrical
t it to an optical signal for insertion
of these functions requires electrical
to sense and control this energy. See also
t doesn't take the light signal back to

: components that turn light energy into
energy.
ctronics.
ically, Australia's second general
1991 to provide competition to then
med from a consortium of Mayne
unications Fund, Bell South and Cable
ork services.
phone terminating in a location other
e circuit out of the PBX. OPX is
xtension off the PBX in his home.
really at home. He can also make

high state if either or both of its inputs are

the U.S. Department of Defense's

powering arrangement for digital

uest Broker and CORBA.
tion which allows someone with a
r.
ne personnel for fixing, installing and

elephone company with the means
carrier repeater locations.
equest, and consisting of one octet

circuit used by telephone company
oordination and control action relating to
ting and maintenance of communication

ow a company's revenues. You can buy
. Or you can grow the revenues in your
products, then marketing and selling
your existing customers. Growing your
usinesses is called organic growth.

te" sets the modem to begin a data phone

i.e. dial the phone, listen for a carrier tone from a remote modem and connect to that modem. The modem at the receiving end must be set to "Answer" mode. In any asynchronous data conversation, one side must be set to "Originate" and the other to "Answer." Such settings are usually made in software.

Originate/Answer The two modes of operation for a modem. Originate and answer states define the frequencies used to transmit and receive. In a two-way communication system, one modem must be set to originate and the other to answer.

Originating Direction The use of Access Service for the origination of calls from an End User premise to a customer premise.

Originating Office The central office that serves the calling party.

Originating Restriction A phone line with this restriction cannot place calls at any time. Calls directed to the phone, however, will be completed normally.

Origination A call that is placed by the mobile subscriber, calling either a land-line unit or another mobile subscriber.

Origination Cablecasting Programming over which a cable television system operator exercises editorial control. This term includes programming produced by the operator; Non-broadcast local programming produced by other entities and carried voluntarily by the system. Example: PRISM; regional news channels; Satellite-delivered non-broadcast programming carried voluntarily by the system, such as HBO, ESPN, CNN, C-SPAN, QVC, etc.

This term does not include programming over which the operator does not exercise editorial control, including any broadcast signal, including satellite-delivered broadcast "superstations" (WGN-TV, WWOR, etc.); Any access channel designated by franchise for public, educational, or governmental use; Leased-access channels.

The cable system operator is required by Section 76.225c of the FCC Rules to maintain records, in the PIF, to verify compliance with rules governing commercial matter in children's programming carried on origination-cablecasting channels. See PIF.

Originator The user that is the ultimate source of a message or probe.

ORM Optically Remote Module. A type of switching module made by AT&T which connects directly to the 5ESS switch communications module via optical fibers.

Orphan A Windows NT term. A member of a mirror set or a stripe set with parity that has failed in a severe manner, such as a loss of power or a complete head crash. When this happens, the fault-tolerance driver determines that it can no longer use the orphaned member and directs all new reads and writes to the remaining members of the fault-tolerant volume.

Orthogonal Having, meeting or determined at right angles.

Orthogonal Frequency Division Multiplexing See OFDM.

OS 1. Outage Seconds.
2. Operating System, as in MS-DOS (Microsoft Disk Operating System), Windows NT, Windows 2000, Windows XP, Solaris, Unix, Linux, Symbian or OS/2. See Operating System.
3. Operator Services. See Operator Services.
4. Operations System. Includes SCOTS, FMAS, etc.

OS/2 Operating System/2. An operating system originally developed by IBM and Microsoft for use with Intel's microprocessors and for use with IBM personal system/2 personal computers. OS/2 has pretty well died. Microsoft's various flavors of Windows survived.

Osborne Effect Once there was a personal computer company called Osborne Computer Company. One day, the president announced a revolutionary new computer. It was so good not one of his dealers wanted to (or could) sell the existing product and they sent all their inventory back. Meantime, it was six months before the company could deliver the new product. But without any sales in the meantime, it had no money and Osborne went broke. There is a lesson here for companies who are attempting to manage transition between old and new product lines. Be careful, or suffer the horrible consequences of The Osborne Effect.

Oscar Hollywood gives our Oscars for great movies, performances, etc. Apparently when the first statue was cast, someone quipped, "My God. It looks like my uncle Oscar." Apparently it stuck.

Oscillator 1. A device for generating an analog test signal.
2. Electronic circuit that creates a single frequency signal.

Oscilloscope Electronic testing device that can display wave forms and other information on a TV-screen-like cathode ray tube. A basic fixture in sci-fi movies.

OSDM Optical Spatial Division Multiplexing is a technology developed to improve the efficiency with which SONET (Synchronous Optical NETwork) supports bursty packet data traffic such as LAN traffic. OSDM accomplishes this by dynamically allocating arbitrary levels of bandwidth to such traffic, guaranteeing minimum levels that are supplemented by higher levels of bandwidth as it becomes available. OSDM is a protocol-independent, self-contained technology that adapts to various current and developing physical layer technologies such as digital wrappers and DWDM (Dense Wavelength Division Multiplexing).

OSF Open Software Foundation. An industry organization founded in 1988 to deliver technology innovations in all areas of open computer systems, including interoperability, scalability, portability and usability. The OSF was an international coalition of vendors and users in industry, government and academia that worked to provide technology solutions for a distributed computing environment. In February 1996, the OSF consolidated with X/Open Company Ltd. to form The Open Group. See The Open Group. www.opengroup.org.

OSF/1 Version 1 of the Open Software Foundation's Unix-based operating system

OSI Open Systems Interconnection. A Reference Model developed by the ISO (International Organization for Standardization, as translated into English). The OSI Reference Model is the only internationally accepted framework of standards for communication between different systems made by different vendors. ISO's goal is to create an open systems networking environment where any vendor's computer system, connected to any network, can freely share data with any other computer system on that network or a linked network. Most of the dominant communications protocols used today have a structure based on the OSI model. Although OSI is a model and not an actively used protocol, and there are still very few pure OSI-based products on the market today, it is still important to understand its structure. The OSI model organizes the communications process into seven different categories and places these categories in a layered sequence based on their relation to the user. Layers 7 through 4 deal with end to end communications between the message source and the message destination, while layers 3 through 1 deal with network access.

OSI Reference Model

Layer 7	Application	Semantics
Layer 6	Presentation	Syntax
Layer 5	Session	Dialog Coordination
Layer 4	Transport	Reliable Data Transfer
Layer 3	Network	Routing & Relaying
Layer 2	Data Link	Technology-Specific Transfer
Layer 1	Physical	Physical Connections

Layer 1 — The Physical Layer deals with the physical means of sending data over lines (i.e., the electrical, mechanical and functional control of data circuits). Examples include EIA-232 (RS-232), T-carrier and SONET.

Layer 2 — The Data Link Layer is concerned with procedures and protocols for operating the communications lines. It also has a way of detecting and correcting message errors. Examples include Frame Relay, PPP (Point-to-Point Protocol), and SLIP (Serial Line Internet Protocol). ATM runs at Layers 1 & 2, as do LANs.

Layer 3 — The Network Layer determines how data is transferred between computers. It also addresses routing within and between individual networks. The most visible example is IP (Internet Protocol).

Layer 4 — The Transport Layer defines the rules for information exchange and manages end-to-end delivery of information within and between networks, including error recovery and flow control. TCP (Transmission Control Protocol) is an example, as is the OSI Transport Protocol (TP), which comprises five layers of its own. Layer 4 protocols ensure end-to-end integrity of the data in a session. The X.25 packet-switching protocol operates at Layers One, Two, Three, and Four.

Layer 5 — The Session Layer is concerned with dialog management. It controls the use of the basic communications facility provided by the Transport layer. If you've ever lost your connection while Web surfing, you've likely experienced a session time-out, so you have some sense of the Session Layer.

Layer 6 — The Presentation Layer provides transparent communications services by masking the differences of varying data formats (character codes, for example) between dissimilar systems. Conversion of coding schemes (e.g., ASCII to EBCDIC to Unicode), and text compression and decompression exemplify Presentation Layer functions.

Layer 7 — The Applications layer contains functions for particular applications services, such as file transfer, remote file access and virtual terminals. TCP/IP application protocols such as FTP (File Transfer Protocol), Simple Mail Transfer Protocol (SMTP), SNMP (Simple Network Management Protocol) and TELNET (TELecommunications Network) take place at Layer 7.

See also OSI Standards, which compares Layers 1 through 2 on OSI to making a phone call on the public switched telephone network. .

OSI Model Open Systems Interconnection Model. See OSI.

OSI Network Address The address, consisting of up to 20 octets, used to locate an OSI Transport entity. The address is formatted into an Initial Domain Part which is the responsibility of the addressing authority for that domain and a domain-specific part which is the responsibility of the addressing authority for that domain.

OSI Presentation Address The address used to locate an OSI Application entity. It consists of an OSI Network Address and up to three selectors, one each for use by the Transport, Session, and Presentation entities.

OSI Standards The International Standards Organization (ISO) has established the Open Systems Interconnection (OSI) Reference Model is to provide a standar network design framework to allow equipment from different vendors to be able to communicate. Standards allow us to buy items such as batteries and light bulbs. Many of us have learned "the hard way" that the lack of computer standards can make it impossible for computers from different vendors to talk to each other. Because a major goal of a LAN (Local Area Network) is to connect varied systems, standards have been developed to specify the set of rules networks will follow. The OSI Model is a design in which groups of protocols, or rules for communicating, are arranged in layers. Each layer performs a specific data communications function. The concept of layered protocols is analogous (but not identical) to the steps we follow in making a phone call:

Step 1 — Listen for dial tone.

Step 2 — Dial a phone number.

Step 3 — Wait for a ring.

Step 4 — Exchange greetings to check that the connection is made and we're speaking the same language.

Step 5 — Talk, i.e. communicate messages back and forth.

Step 6 — Prepare to end conversation. For example, say Goodbye.

Step 7 — Take physical action. Hang up.

Each of these steps, or OSI "layers," builds upon the one below it. Although each step must be performed in preset order, within each layer there are several options. Within the OSI model, there are seven layers. The first three are the Physical (PHY), Data Link (DLL), and Network layers, all of which are concerned with data transmission and routing. The last three — Session, Presentation and Application — focus on user applications. The fourth layer, Transport, provides an interface between the first and last three layers. The X.25 Protocol which created a standard for data transmission and routing is equivalent to the first three layers of the OSI Reference Model." See also OSI and X.25.

OSINet A test network sponsored by the National Bureau of Standards (NBS) designed to provide vendors of products based on the OSI model a forum for doing interoperability testing.

Osmics The science of smells. See Snortal.

OSMINE Operations System Modifications for the Integration of Network Elements. OSMINE enables equipment used by Regional Bell Operating Companies (RBOCs) and other service providers to be managed effectively from the same software program, helping to ensure multi-vendor interoperability.

OSN Operations System Network.

OSP 1. Operator Service Provider. A new breed of long distance phone company. It handles operator-assisted calls, in particular Credit Card, Collect, Third Party Billed and Person-to-Person. Phone calls provided by OSP companies are often more expensive than phone calls provided by "normal" long distance companies, i.e. those which have their own long distance networks and which you see advertised on TV. You normally encounter an OSP only when you're making a phone call from a hotel or hospital phone, or privately-owned payphone. It's a good idea to ask the operator what the cost of your call will be before you make it.

2. Online Service Provider. A company that provides content only to subscribers of the service. This content is not available to regular Web surfers. The idea was to [illegible] subscription and other revenues from a closed knit group of people. The problem with this [illegible] was the Internet came along and no one any longer could afford a team to compete with the Web's exploding and varied content. So, some online service providers dropped the attempt at content altogether. Others severely limited it. But all were forced to offer (and do offer) access to the Internet. As a result the term "online service provider" has [illegible]ly become obsolete, to be replaced by the term, Internet Service Provider.

OSPF Open Shortest Path First. My definition is that OSPF is a link-state routing algorithm that is used to calculate routes based on the number of routers, transmission speed, delays and route cost. Here's a longer explanation from Alcatel:

Open Shortest Path First (OSPF) as described in RFC 1245 and RFC 1583 is a routing protocol designed for larger or more complex networks than those typically supported by the Routing Information Protocol (RIP). OSPF uses link state and interior gateway protocols to create a network map on each router and then uses the Dijkstra shortest path algorithm to find the optimum path between network devices. RIP has visibility only to the next hop and uses the distance vector algorithm.

Link state protocol algorithms determine the state of, or status of, each link connected to the router. In a network each router constructs a link state advertisement (LSA) with the status of its links and transmits this to its neighbors. Each router builds a list of all routes to all destinations, based on the compilation of LSAs from each router. Each router identifies which routers and subnets are directly connected to it. Then, it distributes this information to all other routers. OSPF routers take the information and build a table of what the network looks like. Using this table, each router can identify where the subnetworks are located, what routers are in direct connection, and how to get to any specific [illegible].

As an interior gateway protocol, OSPF distributes routing information between routers in a single autonomous system. Once all routers have constructed their databases based on the LSA information, they run the Shortest Path First Algorithm. This results in a tree structure with each router at the "root" of its own tree, and the shortest path to all other destinations mapped out. The selection of the path to these destinations is based on metrics. These metrics may be based on hop count, bandwidth, load, cost, reliability, delay, or controlled statically by the user. This provides the network manager greater control over how routing occurs in the network. Dijkstra's Shortest Path Algorithm is a mathematical [illegible] by which it is possible to find the shortest path between points. Essentially, the Dijkstra Shortest Path Algorithm calculates the cost of a path between points beginning with the closest points to the starting point and works its way outward until it reaches the [illegible] end point. A high bandwidth link costs less because more information can be sent across at one time. Conversely, a lower speed/smaller bandwidth connection costs more because it is not able to send information as quickly. For instance, when sending packets across a 56k point-to-point serial connection there is more delay and overhead than if the same packet was sent over a 100Mbps Ethernet connection. Therefore, it would cost more [illegible] to send a transmission over the 56k connection compared to the 100Mbps connection.

OSPF is an excellent protocol in a larger network because it can build a map of large complex networks and then navigate a path between two of the network devices with visibility of the entire network providing the most efficient routing paths possible. Because of its ability to handle large complex networks, OSPF can be complex for the network manager to configure and set up and requires greater computing power within the [illegible]. However, OSPF is often the routing protocol of choice when configuring larger networks due to its ability to quickly adapt to network changes (faster route convergence), [illegible] network metrics, area-based topology, low traffic overhead and the ability to support complex address structures and route summarization. Such speed and efficiency [illegible] mized bandwidth usage, faster routing compared to other comparable protocols (RIP, RIPv2), lower network latency and better overall network performance, which is especially useful in networks where bandwidth is at a premium such as in a WAN.

OSPFIGP Open Shortest-Path First Internet Gateway Protocol. An experimental replacement for RIP. It addresses some problems of RIP and is based upon principles that have been well-tested in non-internet protocols. Often referred to simply as OSPF. See OSPF.

OSPR Optical Shared Protection Ring.

OSPS An AT&T word for Operator Services Position System.

OSS Operations Support System. Methods and procedures (mechanized or not) which directly support the daily operation of the telecommunications infrastructure. The [illegible]